REMARKS

Reconsideration of the application is respectfully requested for the following reasons:

1. Rejections of Claims 18-32 Under 35 USC §102(e) and of Claim 33 Under 35 USC §103(a) in view of U.S. Patent No. 6,442,600 (Anderson)

This rejection is respectfully again traversed on the grounds that the Anderson patent does not disclose the feature wherein a message can **only** be viewed before a designated expiration date by a viewer applet installed on the **recipient's** computer. While it is true that system of Anderson provides a message distributor that controls distribution of messages to recipient's using the system disclosed therein, that can encrypt and decrypt messages, and that can implement an expiration date by setting an entry in a message tracking table and deleting the message at the expiration date, the system of Anderson does not seek to control messages that have already been sent to the recipient's computer. **The messages deleted in response to the "Message Tracker" of Anderson are those save by the "Message Distributor" and not messages that have already been accessed by a recipient.** Without a viewer applet on the recipient's computer, the system of Anderson cannot force expiration of a message in all its incarnations, as claimed, because Anderson does provide any software (the claimed viewer applet) on the recipient's computer. Once the recipient has obtained a copy of the message, the system of Anderson cannot force expiration..

As explained in the abstract of the Anderson patent:

> *After a recipient receives an indicator, the recipient can use the indicator to access and review the message. The **recipient** can also provide various instructions about actions to be taken with the message corresponding to an indicator, such as to save or delete the message or to forward the message to another recipient. After all recipients have reviewed the message and **no recipient has currently indicated to save the message** (or all have indicated to delete the message), the system can then delete the single copy of the message.*

It is the RECIPIENT that controls ultimate expiration of the message. While the server will clear or delete any messages from storage by a designated expiration date, any recipient

attached to the local mail server can elect to at least access a message before expiration, and take control of the message. Once a message is accessed, then the recipient can do whatever it wants with the message.

The claimed invention operates by user applet installed on the recipient's computer to **prevent viewing** of a message unless message handling limitations that are set by the message **originator** (sender) are implemented. This is accomplished by encrypting the message and controlling viewing by an applet that only decrypts the message until the expiration date, after which it stops decrypting the message. In the system disclosed in the Anderson patent, all message handling instructions are implemented by a tracking table and central message distributor, and the recipient is, in general, left with the option of viewing, saving, decrypting, and so forth a message without reference to the wishes of the message originator.

It is true that in the system of Anderson, the sender's local mail server (Message Sender) can be instructed by the sender to carry out encryption. However, this encryption is not used to prevent viewing of a message after a sender-designated expiration date. Instead, the "maximum time expiration period for the message" referred to in col. 7, line 25, causes the "Message Tracker" to delete the message from storage by the "Message Distributor." **By the time this has occurred, the Message Distributor has already either stored the message in decrypted form on the "Message Receiver" (a local server) or decrypted the message when accessed by a recipient, so that the recipient can access the message whenever desired (col. 6, lines 25).**

According to the claimed invention, the message originator can set an expiration date for the message, in which case **all incarnations of the message, no matter to whom the message is forwarded or who accesses the message,** will expire because the viewer applet will prevent the message from being viewed by any recipient after the expiration date. The reason that the recipient cannot view the message after the expiration date is that the

message is encrypted, and can only be decrypted and viewed using the "viewer applet." If the viewer applet is set to prevent decryption of the message after the expiration date, then the message simply cannot be viewed. Similarly, if the message originator wishes to limit printing of the message, then the viewer applet can be set to prevent printing of the message. If the recipient attempts to print the message without using the viewer applet, the result will be printing of an unencrypted message.

Of course it might be possible for a sophisticated recipient to try to decrypt the message by means other than the viewer applet. However, according to a further feature of the invention, positively recited in claims 2, 19, 34, 38, and 42, the message is kept on a central server and streamed to the viewer applet, so that the recipient never has access to the entire message file, even in encrypted form. This further limits recipient access to the message, and enables certain controls to be implemented at the central server level rather than by execution of instructions on the recipient's computer, thereby providing a further degree of control or security.

In contrast, Anderson provides a means for enabling recipients to better control message viewing. In particular, the Anderson patent discloses a system that notifies a **recipient** that a message is available, and then gives the **recipient** the option of viewing, encrypting, saving, and/or deleting the message. While Anderson does provide for some control of message viewing duration, the duration is controlled by a "message tracking table" which is only capable of deleting any messages saved by the "Message Distributor," ***and the control of duration is carried out irrespective of whether the message is encrypted.***

The purpose of the system of Anderson is to save **recipients** the trouble of storing, managing, and protecting received messages, as explained in col. 1, lines 20-29 and in particular in col. 1, lines 65 *et seq.* of the Anderson patent.

> *Some embodiments of the present invention provide a method and system for distributing electronic messages in an efficient manner using centralized storage and management. In particular, the system receives electronic messages*

> *to be distributed to one or more recipients, centrally stores a single copy of the message as well as various information about sending the message, and sends to each recipient a short indicator message to notify the recipient that the electronic message is available. The system then tracks and manages requests from the recipients to access the message by permitting access when appropriate, performing activities such as decrypting/encrypting the message if necessary, recording information about the access and about recipient instructions related to the message, archiving the message if necessary, and deleting the message when it is no longer needed. The recipient can also provide various instructions about actions to be taken with the message corresponding to an indicator, such as to save or delete the message or to forward the message to another recipient. In one embodiment, after all recipients have reviewed the message and no recipient has currently indicated to save the message (or all have indicated to delete the message), the system then deletes the single copy of the message).*

Nowhere does this passage disclose or suggest that tracking and management of messages is in response to controls selected by the originator or sender of the message **and implemented by means of encryption and a viewer applet on the recipient's computer**

To implement the system of Anderson, there is no need for a special "viewer applet" that limits message access by the recipient. The only encryption provided for is encryption at the request of the recipient to limit viewing by third parties. There are no limits on viewing of the message by the recipient, and any limitations that are selected by the message originator or sender are implemented by a message tracking table rather than a viewer applet, as claimed, that decrypts the message at the recipient's computer.

Because the Anderson does not disclose or suggest an electronic mail system that implements controls selected by the originator of the message rather than intended recipients, **using a viewer applet installed on the recipient's computer** to implement the originator-selected controls by preventing decryption of the message unless the controls are implemented, it is respectfully submitted that the rejections of claims 1-50 based on 35 USC§102(e) and 103(a) are improper and should be withdrawn.

2. Rejections of Claims 1-17 and 34-50 Under 35 USC §103(a) in view of U.S. Patent No. 6,442,600 (Anderson) and U.S. Patent Publication No. 2003/1026215 (Udell)

This rejection is respectfully traversed on the grounds that the Udell publication, like the Anderson patent, fails to disclose or suggest the claimed viewer applet that enables reading of an e-mail message **using the viewer applet**, and yet that prevents viewing of the message after the expiration date of the message **by preventing decryption**. Udell attaches a virus to the message, which causes the user's system to destroy the message, while Anderson's system relies on software controlled entirely by the recipient to cause expiration. The claimed invention, on the other hand, allows the **sender** to control expiration, and yet does not require the sender to attach any executable code to the message, but rather uses a viewer applet to enable reading of a message until the preset date sent by the user. Each of the patents applied by the Examiner effectively causes message expiration, but neither does it in the claimed manner.

The differences may be summarized in the following table:

	Claimed	Anderson	Udell
Who Controls Expiration?	Sender, central server, viewer applet on recipient's computer	Sender, tracking table associated with central Message Distributor–no applet on recipient's computer	Sender, virus or "applet" attached to message itself
How is Expiration Implemented?	Viewer applet is used to decrypt and view message until expiration date–applet then stops decrypting and displaying message	Tracking table causes deletion of message from central storage at expiration date	Virus ("applet") attached to message by sender and destroys message at expiration date–virus does NOT decrypt or display message

Can sender control forwarding, copying, etc.?	Yes, since viewer applet on recipient computer controls both message viewing and handling, it can be set to implement any controls	No	No
Does central server encrypt message?	Yes, if recipient wishes to view message, it is encrypted and streamed to recipient–otherwise, recipient does not receive message	Yes, but once decrypted, recipient controls message	Message can be encrypted by sender, but encryption has nothing to do with operation of the virus to destroy message at expiration date.

The approach taken by the Udell publication is contrary to that of the invention, and involves a virus attached to the message that destroys the message at the expiration date. While the Examiner is correct that a virus can be termed an "applet," the claimed applet does not function in the same manner as the virus or "applet" of Udell. The claimed invention does not attach the applet so that it follows the message wherever it might be sent or forwarded. Instead, the claimed applet is a viewer that is used to read a message by decrypting it. Claim 1 specifically recites that the message is "**encrypted so that it may only be viewed by a recipient *using said viewer applet* upon installation of said viewer applet on said at least one recipient computer**." The applet of Udell is not used to read an encryption message. It simply is attached to the message and, at a predetermined time, destroys the message.

The claimed invention does not seek to destroy a message, but rather operates by supplying a recipient that permits reading of a message until the preset time has expired. The message is not necessarily destroyed. Instead, the viewer stops enabling the message to be read. Since the message is encrypted and can only be read by the viewer, once the

viewer stops reading the message, the effect is as if the message has expired. This is a fundamentally different, *and more secure*, approach than that used by Udell because expiration of the message does not depend on attachment of executable code.

There are a number of problems with the approach taken by Udell. The first is that there is nothing to prevent copying, forwarding, and printing of the message is the usual manner. Udell provides for the virus to be forwarded with the message, but cannot stop the message from being forwarded or printed. Second, and probably more important from a practical standpoint, most firewalls prevent executable code from being transmitted with e-mail messages. The claimed invention does not have this problem because the message contains no executable code, and will not be tagged or blocked by a firewall or antivirus software. The message of the claimed invention is an ordinary, albeit encrypted, e-mail message can be received like an ordinary message (or streamed to a browser as recited in claims 2 and 4, as discussed below) in the sense that it does not carry executable code. The applet used to read the message according to the principles of the claimed invention is a separate entity.

The recitation in claim 1 that the applet is used to decrypt and view the message clearly distinguishes it from the virus of Udell. The virus of Udell neither decrypts nor is used to view the message. It merely destroys the message.

Furthermore, neither the Anderson nor Udell patents suggests the use of a central server to **stream** messages to an expiration-date controlling viewer applet on the recipient's computer. As explained above, the Anderson patent discloses deletion of a saved message by a central "tracking table" associated with a "message distributor." Prevention of viewing is not carried out by a viewer applet on the recipient's computer. This is not only contrary to the claimed invention, but also fundamentally different than the approach taken by Udell, in which the central server that forwards e-mail plays no part in the message expiration

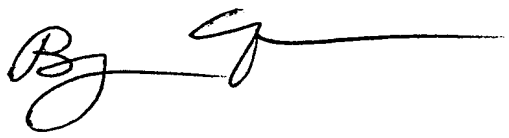
and/or control, message expiration being controlled solely by a virus attached to the message.

Because neither the Anderson patent nor the Udell patent discloses or suggests control of message expiration by means of a viewer applet on the recipient's computer that provides access to the message prior to the expiration date through the use of decryption, and that prevents such access by ceasing decryption after the expiration date, withdrawal of the rejection under 35 USC §103(a) is respectfully requested.

Having thus overcome each of the rejections made in the Official Action, expedited passage of the application to issue is requested.

Respectfully submitted,

BACON & THOMAS, PLLC



Date: May 24, 2004

By: BENJAMIN E. URCIA
Registration No. 33,805

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314
Telephone: (703) 683-0500

NWB:SAProducer\beu\Pending L...PULEONARD390363\a02.wpd